ELSEVIER

computer
FRAUD & SECURITY

ISSN 1361-3723 October 2020 www.computerfraudandsecurity.com

Featured in this issue:

Moving from blocker to enabler: cloud security and the modern CISO

The role of the chief information security officer (CISO) is changing. It's an exciting time for many as the new world of public cloud comes to fruition.

But change often brings fear and anxiety, and it's not unusual for the IT security function to act as 'blockers'. Yet with the right changes, modern CISOs can act as a springboard to demonstrate relevance and the importance of their role while shaping a more secure IT landscape, says Olivier Subramanian of Contino.

Full story on page 6…

How to leverage data security in a post-Covid world

Cyber security is often pushed down the list of priorities and this became abundantly clear as businesses had to rush to get employees up and running when working from home in recent months.

With a lasting switch to remote working and changing work habits and practices, there must be a refreshed emphasis on data security. The new normal of hybrid workforces must have the correct layers of security that protect all types of employees. It's about increasing awareness and improving email culture, argues Andrea Babbs of Vipre Security.

Full story on page 9…

PKI is key to securing a post-Covid remote workforce

With the Covid-19 outbreak, analysts estimate that we have witnessed two years of IT digital transformation in two months, and many of the changes are here to stay.

Most organisations were forced to shift employees to remote work in just weeks or even days. The switchover has opened the door to a flood of new security threats. Multifactor authentication, such as PKI certificates and passwords, is the best approach to apply flexible, scalable security to protect networks and their users in today's world, explains Brian Trzupek of DigiCert.

Full story on page 12…

Ransomware claims first fatality as healthcare under renewed assault

Ransomware has claimed its first death after a German hospital was unable to treat a woman requiring critical care. And the US Government has warned organisations that paying ransoms could put them in breach of regulations.

German authorities have opened a 'negligent homicide' investigation after a woman who was scheduled to undergo critical treatment at Düsseldorf University Clinic (DUC) was unable to be admitted because of an ongoing ransomware attack –

Continued on page 3...

Contents

NEWS

FEATURES

REGULARS

...Continued from front page

believed to be caused by the DoppelPaymer malware that had entered the system through a vulnerability in Citrix software (CVE-2019-19781). The woman had to be transported to another hospital 30km away. It's believed that the delay of an hour contributed to her death.

It appears as though the clinic was not the intended target. Heinrich Heine University, with which DUC is affiliated, was the institution the criminals intended to attack. However, somehow the malware found its way on to 30 of DUC's servers. A ransom note found on one of those servers was addressed to Heinrich Heine University.

Police officers contacted the attackers via the details in the ransom note and explained that the hospital had been hit. The criminals provided a decryption key and made no further attempt to extort money.

DUC said that no data had been irretrievably lost and a week after the attack systems were coming online again.

Universal Health Services (UHS), one of the biggest hospital and healthcare services providers in the US, has suffered a major nationwide ransomware attack that has affected dozens of its facilities. UHS hospitals in California, Florida, Texas, Arizona and Washington DC – and possibly many other locations – were left without access to computer and phone systems.

The firm operates over 400 healthcare facilities in the US and UK, employs more than 90,000 people and provides healthcare services to around 3.5 million patients a year. It hasn't offered any details about the nature of the attack, although a number of its employees took to Reddit to confirm that facilities were impacted with what appears to be the Ryuk strain of ransomware. Advanced Intel said that it had monitored Emotet and TrickBot attacks against UHS throughout 2020, and Trickbot is notorious for providing a reverse shell to the Ryuk operators.

According to Jamie Akhtar, CEO and co-founder of CyberSmart: "This is an absolute tragedy – but not an entirely unexpected one. The healthcare industry with its already stretched resources has continued to be an enormous target for cyber criminals since Covid lockdowns began. When we speak about the healthcare industry we aren't just talking about hospitals and computers full of medical records. The healthcare system is possibly the most complex supply chain in our economy."

UHS issued a statement that said: "We implement extensive IT security protocols and are working diligently with our IT security partners to restore IT operations as quickly as possible. In the meantime, our facilities are using their established back-up processes, including offline documentation methods. Patient care continues to be delivered safely and effectively."

However, some workers have told media outlets that they have had to revert to paper-based processes.

There has also been an attack on a tech company that supplies software used in clinical trials. The New York Times reported that Philadelphia-based eResearchTechnology (ERT) was hit with ransomware a couple of weeks ago. This has had a knock-on effect with many of its customers, a number of which are involved in clinical trials for Covid-19 vaccines and treatments. The company has declined to state whether it paid the ransom but has claimed that no patients have been affected.

The New York Times report is here: https://nyti.ms/2F9f90E.

It's been reported that University Hospital New Jersey in Newark paid a $670,000 ransomware demand to stop criminals from publishing 240GB of stolen data, including patient information. The hospital was hit in September by an outfit known as SunCrypt.

However, making such payments could get US-based organisations into deeper trouble. The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury said: "Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

The Department of the Treasury has imposed sanctions on a number of individual cyber criminals and cybercrime groups. Before dealing with sanctioned entities, organisations need to obtain a licence: paying the criminals without doing so is a breach of those sanctions and could incur significant penalties – as much as $20m.

OFAC's advisory is here: https://bit.ly/30Bo1DS.

FBI makes 179 arrests in dark web sting

An FBI-led operation lasting nine months has resulted in major drug busts on dark web marketplaces.

Operation DisrupTor led to 179 arrests in seven countries and the seizure of $6.5m in cash and crypto-currency, 500kg of illegal drugs and 63 guns. The drugs consisted mainly of opioids such as fentanyl, oxycodone and hydrocodone although methamphetamine, heroin, cocaine and ecstasy were also found.

Working with the FBI were the Drug Enforcement Agency (DEA), Department of Homeland Security, the Secret Service, the Postal Inspection Service, the Inland Revenue Service (IRS), and the Bureau of Alcohol, Tobacco and Firearms (ATF). In addition, Operation DisrupTor involved law enforcement agencies in several other countries. The arrests were made in the US (121), Germany (42), the Netherlands (8), the UK (4), Austria (3), Canada (2) and Sweden (1).

Several dark web markets were targeted, including AlphaBay, Dream, Wall Street, Nightmare, Empire, White House, DeepSea and Dark Market. The investigators were able to identify and locate vendors using the markets.

Dark web markets use the Tor anonymising service in an effort to hide the location of the servers and the people – both vendors and customers – using the sites. However, this isn't the first time that law enforcement operations have subverted that anonymising process – previous operations such as SaboTor in 2019, which focused on the Wall Street Market – did the same. No information has been offered as to how the authorities overcame the protection offered by Tor.

There's more information here: https://bit.ly/33CBNYO.